UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/757,742	01/13/2004	Peter Szor	20423-08312	4893

34415 7590 07/06/2007

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2136	

NOTIFICATION DATE	DELIVERY MODE
07/06/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	Application No.	Applicant(s)	
	10/757,742	SZOR ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9,12,14,19-22 and 24-28* is/are rejected.

7)☒ Claim(s) *8,10,11,13,15-18,23 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 17 January 2006.

2. Claims 1-29 are pending for examination.

3. Claims 1-7, 9, 12, 14, 19-22 and 24-28 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-7, 9, 12, 14, 19-22 and 24-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Arnold et al, U.S. Patent No. 6,981,279 B1.

5. As per claim 1; "A computer implemented method for preventing malicious code from propagating in a computer, the method comprising the steps of:

a blocking-scanning manager

detecting attempted malicious behavior of running code [*Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, (inclusive of malicious behavior client applications) such that said software can be executed (i.e., generated/loaded/running) in a real or emulated network environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

responsive to the detection, the blocking-scanning manager

blocking the attempted malicious behavior [*Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that said software 'being analyzed is effectively confined to the analysis network ... and cannot in fact read information from, or alter any ... production ... global Internet' (i.e., col. 2,lines 23-39) is effectively blocked from any 'attempted malicious behavior', clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

the blocking-scanning manager

generating a signature to identify

the code that attempted the malicious behavior [*Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the monitoring component 'serves to capture and/or record the behaviors ...' (i.e., col. 2,lines 23-39) is effectively 'generating a signature to identify' of any 'attempted malicious behavior', clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

the blocking-scanning manager

detecting code identified by the signature [*Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the actual detection/run in an emulated environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*]; and

the blocking-scanning manager

blocking the execution of the identified code [*Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the actual detection/run in an emulated environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*].".

As per claim 19, this claim is the system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A computer system for preventing the propagation of malicious code, the computer system comprising:

a running code detection module,

configured to detect

attempted malicious behavior of running code;

a running code blocking module,

configured to block

the attempted malicious behavior in response to positive detection,

the running code blocking module being

communicatively coupled to

the running code detection module;

a signature module,

configured to generate

a signature to identify the code that attempted the malicious behavior,

the signature module being

communicatively coupled to

the running code blocking module;

an scanning module,

configured to detect

code identified by the signature,

the scanning module being

communicatively coupled to

the signature module; and

an identified code blocking module,

configured to block

the execution of the identified code,

the identified code blocking module being

communicatively coupled to

the scanning module.".

As per claim 25, this claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A computer-readable medium containing a computer program product for preventing the propagation of malicious code in a computer, the computer program product comprising:

program code for a blocking-scanning manager

detecting an attempted malicious behavior of a running code;

program code for the blocking-scanning manager

blocking the attempted malicious behavior in response to the detection;

program code for the blocking-scanning manager

generating a signature to identify the code that attempted the malicious behavior;

program code for the blocking-scanning manager

detecting code identified by the signature; and

program code for the blocking-scanning manager

blocking the execution of the identified code.".

6. Claim 2 *additionally recites* the limitations that; "The method of claim 1 wherein

a source of at least one of

the running code and

the identified code

comprises

a source from a group of sources consisting of

an e-mail attachment,

a magnetic medium,

an optical medium,

a file,

a boot sector, and

a network remote computer.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing

software, such that the monitoring (of the running/identified code) component encompasses 'receipt of [E]mail …' (i.e., col. 2,lines 57-col. 3,line 3), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

7. Claim 3 *additionally recites* the limitations that; "The method of claim 1 wherein

the blocking-scanning manager

detecting code identified by the signature further comprises

the blocking-scanning manager

comparing

the running code to

at least one signature generated.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the monitoring component 'serves to capture and/or record the behaviors …' (i.e., col. 2,lines 23-39), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

As per claim 21, this claim is the system claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The computer system of claim 19, wherein

the scanning module

is further configured to compare

running code to

at least one signature generated,

the scanning module being

communicatively coupled to

the signature module.".

As per claim 26, this claim is the embodied software claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The computer program product of claim 25, further comprising

program code for

the blocking-scanning manager

comparing

the running code to

at least one signature generated.".

8. Claim 4 *additionally recites* the limitations that; "The method of claim 3, wherein

the blocking-scanning manager

comparing the running code to at least one signature generated further comprises

the blocking-scanning manager

determining

that the running code matches

at least one of the generated signatures.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the monitoring component 'serves to capture and/or record the behaviors …' (i.e., col. 2,lines 23-39), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

9. Claim 5 *additionally recites* the limitations that; "The method of claim 1 wherein

the blocking-scanning manager

detecting code identified by the signature further comprises

the blocking-scanning manager

placing at least one of

the running code and

the identified code

in a repository, such that

the user cannot execute the code.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that said software 'being analyzed is effectively confined to the analysis network … and cannot in fact read information from, or alter any … production … global Internet' (i.e., col. 2,lines 23-39) is effectively blocked (in the emulated environment) from any execution of any running/identified code, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

As per claim 20, this claim is the system claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; "The computer system of claim 19, further comprising

a repository,

configured to store at least one of

the running code and

the identified code,

such that the user cannot execute the code,

the repository being

communicatively coupled to

the running code detection module and

the scanning module.".

10. Claim 6 *additionally recites* the limitations that; "The method of claim 1 further comprising:

the blocking-scanning manager

performing the detecting step on

a first computer able to connect to a network;

the blocking-scanning manager

placing at least one of

the running code and

the identified code

in a repository located

at a location from a group consisting of

locally on the first computer, and

remotely on

a second computer able to connect to the network; and

the blocking-scanning manager

performing the blocking step

at a location from a group consisting of

locally on

the first computer or

remotely on

a second computer able to connect to the network.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the various detecting, analyzing, emulating network nodes and associated functionality, clearly are configurable across a multiple node network (i.e., client/server, P2P, etc.,), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

11. Claim 7 *additionally recites* the limitations that; "The method of claim 1 wherein detecting code identified by the signature further comprises:

the blocking-scanning manager

alerting a user of the detection; and

the blocking-scanning manager

allowing the user to choose whether or not

to block the execution of the identified code.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that said software 'being analyzed is effectively confined to the analysis network ... and cannot in fact read information from, or alter any ... production ... global Internet' (i.e., col. 2,lines 23-39) is effectively blocked (in the emulated environment, as per the network operator/users (i.e., alerting a user of the detection)) from any execution of any running/identified code, clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

As per claim 22, this claim is the system claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection; "The computer system of claim 19, further comprising

an alert module,

configured to

alert a user of detection of

attempted malicious behavior of code,

wherein the alert module is further configured to

allow a user to choose whether or not

to block the execution of the code,

the alert module being

communicatively coupled to

the running code detection module and

the scanning module.".

As per claim 28, this claim is the embodied software claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection; "The computer program product of claim 25, further comprising:

program code for

a blocking-scanning manager

alerting a user of detection of

attempted malicious behavior of code; and

program code for

a blocking-scanning manager

allowing a user to choose whether or not

to block the execution of the code."

12. Claim 9 *additionally recites* the limitations that; "The method of claim 1 further comprising

the blocking-scanning manager

regulating the number of signatures

generated within a period of time.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the monitoring component 'serves to capture and/or record the behaviors …' (i.e., col. 2,lines 23-39) is effectively 'regulating the number of signatures' by virtue of the fact that the analysis/emulation cycle per se is done inherently 'within a period of time', clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

As per claim 24, this claim is the system claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection; "The computer system of claim 19, further comprising

a signature regulation module,

configured to regulate the number of signatures

generated within a period of time,

the signature regulation module being

communicatively coupled to

the signature module.".

13. Claim 12 *additionally recites* the limitations that; "The method of claim 1 wherein the blocking-scanning manager blocking

the execution of the identified code further comprises

the blocking-scanning manager

associating a name with the identified code.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the analysis/emulation component encompasses dealing with DNS, WINS, etc., which are clearly name-associated node/functionality (i.e., and therefore associated identified code), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

As per claim 27, this claim is the embodied software claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection; "The computer program product of claim 25, further comprising

program code for

the blocking-scanning manager

associating a name with the identified code.".

14. Claim 14 *additionally recites* the limitations that; "The method of claim 1 wherein

the blocking-scanning manager

generating a signature to identify the code that

attempted the malicious behavior further comprises:

the blocking-scanning manager

applying a checksum function to generate a checksum of

the code that attempted the malicious behavior;

the blocking-scanning manager

storing the checksum; and

the blocking-scanning manager

using at least one stored checksum

to identify code that attempted malicious

behavior.".

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 1,line 63-col. 3,line 5, col. 9,lines 46-col. 12,line 64, whereas the method for dynamically analyzing software, such that the monitoring component 'serves to capture and/or record the behaviors …' (i.e., col. 2,lines 23-39) is effectively 'generating a signature to identify the code' by virtue of the fact that the analysis/emulation deals with various functions/protocols (i.e., WEB, DNS, WINS, etc.,) that inherently process/generate/store checksums as part of the functionality(i.e., building a header for a WEB HTTP packet), clearly encompassing the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

Allowable Subject Matter

15. Claims 8, 10, 11, 13, 15-18, 23 and 29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

16. Claim 8 *additionally recites* the limitations that; "The method of claim 7 further comprising

the blocking-scanning manager

overriding the user's choice

responsive to the user

incorrectly choosing to block

non-malicious behavior or

incorrectly choosing not to block

malicious behavior.".

As per claim 23, this claim is the system claim for the method claim 8 above, and is objected to for the same reasons provided for the claim 8 objection; "The computer system of claim 22, wherein

the alert module is further configured

to override the user's choice

responsive to the user

incorrectly choosing to block

non-malicious behavior or

incorrectly choosing not to block

malicious behavior.".

As per claim 29, this claim is the embodied software claim for the method claim 8 above, and is objected to for the same reasons provided for the claim 8 objection; "The computer program product of claim 28, further comprising

program code for

a blocking-scanning manager

overriding the user's choice

responsive to the user

incorrectly choosing to block

non-malicious behavior or

incorrectly choosing not to block

malicious behavior.".

17. Claim 10 *additionally recites* the limitations that; "The method of claim 9 wherein regulating the number of signatures further comprises:

the blocking-scanning manager

recognizing a predetermined limit on

the number of signatures

generated within a period of time;

responsive to reaching the predetermined limit,

the blocking-scanning manager

removing older signatures

as newer signatures are generated".

18. Claim 11 *additionally recites* the limitations that; "The method of claim 9 wherein regulating the number of signatures further comprises:

the blocking-scanning manager

sorting the signatures according to

number of matches per signature to

running code that attempted malicious behavior; and

responsive to reaching the predetermined limit,

the blocking-scanning manager

removing the signatures

with the fewest matches

as newer signatures are generated.".

19. Claim 13 *additionally recites* the limitations that; "The method of claim 12 wherein associating a name with the identified code further comprises

the blocking-scanning manager

changing the name to accord with

a new definition of the identified code

in a database of known malicious code.".

20. Claim 15 *additionally recites* the limitations that; "The method of claim 1 wherein the blocking-scanning manager

generating a signature to identify the code that

attempted the malicious behavior further comprises:

the blocking-scanning manager

applying a hash function to generate a hash of

the code that attempted the malicious behavior;

the blocking-scanning manager

storing the hash; and

the blocking-scanning manager

using at least one stored hash

to identify code that attempted malicious

behavior.".

21. Claim 16 *additionally recites* the limitations that; "The method of claim 15 wherein the blocking-scanning manager

applying a hash function to generate a hash further comprises

the blocking-scanning manager

generating a hash of at least a portion of

a code segment of computer-readable contents

associated with the code.".

22. Claim 17 *additionally recites* the limitations that; "The method of claim 15 wherein the blocking-scanning manager

applying a hash function to generate a hash further comprises

the blocking-scanning manager

generating a hash of at least a portion of

a data segment of computer-readable contents

associated with the code.".

23. Claim 18 *additionally recites* the limitations that; "The method of claim 15 wherein the blocking-scanning manager

applying a hash function to generate a hash further comprises

the blocking-scanning manager

generating a hash of at least a portion of

a header of computer-readable contents

associated with the code.".

Conclusion

24. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6/27/07